Department of Homeland Security Daily Open Source Infrastructure Report for 28 December 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a mass transit driver for Broward County Transit in south Florida was arrested Monday, December 26, after he allegedly threatened to blow up a bus. (See item 12)
- The Washington Times reports U.S. Customs and Border Protection has targeted the Del Rio, Texas, sector for a multi−agency border−control initiative called "Operation Streamline II," which will focus on high−traffic smuggling corridors along the 205 miles of the Rio Grande that divide the sector from Mexico. (See item 13)
- Reuters reports China will begin mass−production of a new bird flu vaccine for poultry by the end of the month that could also help in the development of a vaccine to protect people. (See item 23)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *December 27, Palatka Daily News (FL)* — **Man dies in explosion at power plant.** A Georgia man working with as industrial cleaning contractor died Saturday, December 24, after an accident at Seminole Generating Station in Palatka, FL, according to Seminole spokesperson

Michele A. Collet−Kriz. Precision Blasting, Inc., was in Palatka using explosives to de−slag the Unit 2 boiler, said Collete−Kriz. De−slagging is a process of removing burn material from the inner walls of the boiler. “Whenever a power plant burns fuel, a substance called slag sticks to the walls,” said Tim Lutz, safety and compliance director for Precision Blasting, Inc. “When maintenance needs to be done, we have to remove the slag first,” he added. The Occupation Safety and Health Administration was in Palatka Saturday and Sunday, December 25, and would return January 4 to conclude their investigation.
Source: http://www.palatkadailynews.com/articles/2005/12/27/news/new s03.txt

2. *December 27, UPI* — **Blast causes UK gasoline shortage.** A blast this month at a fuel terminal in Britain has begun to disrupt gasoline supplies but as yet there is no panic buying. Motorists are feeling pinch as gas stations struggle to cope with the effects of the Buncefield depot blast. The shortage has been aggravated by high demand in the run−up to Christmas. Fuel retailers say some garages in southeast England have run out of gasoline and others are running short, but retailers are confident they can restock the garages in the next couple of days.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20051227−12595 7−1228r

3. *December 27, Associated Press* — **Shortage of workers slows Gulf oil recovery.** Enough work, not enough workers is a familiar refrain among companies supporting the Gulf's oil and gas industry. It underscores one of several major problems the industry faces as it struggles to rebuild a complex web of platforms, pipelines and processing plants before the next hurricane season arrives. With demand outstripping supply for everything from inspection and repair crews to supply ships to power tools, the price for all of these things is going up. Also on the rise are wait times for some much−needed oilfield services and equipment as competing oil and gas producers sign longer than usual contracts in order to avoid finding themselves at the back of the line. Even when all the best crews and equipment are available, it is slow going. To be sure, oil and gas producers have made significant progress in restoring production in spite of these challenges. Still, about a quarter of the Gulf's daily oil output, and one−fifth of its natural gas output, remains offline and the pace of progress is expected to slow in the months ahead, a trend that could keep upward pressure on energy prices.
Source: http://www.buffalonews.com/editorial/20051227/1025206.asp

4. *December 26, Reuters* — **Agency formally concludes government oil stock release.** The International Energy Agency (IEA) has formally ended a program to release government−held oil stocks in the wake of U.S. Gulf Coast hurricanes, most of which had been sold in September, the agency said. The IEA, energy adviser to 26 industrialized nations, authorized the release of 60 million barrels of oil −− estimated at two million barrels daily −− on September 2 to keep markets well supplied with crude and fuels after Hurricane Katrina ripped up U.S. Gulf production platforms and tore into coastal refineries. While most countries concluded their sales in the first four or six weeks, the IEA had agreed to leave the offer open in order to keep any leftover supplies available to the market. It was the group's first coordinated release in 15 years.
Source: http://www.nytimes.com/reuters/business/business−energy−stoc ks−release.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *December 27, Associated Press* — **Fuel, kerosene heater start deadly rowhouse fire in Philadelphia.** Fuel stored near a kerosene heater combined to set off a rowhouse fire in North Philadelphia, PA, that left one man dead, authorities said. The fuel was stored in plastic jugs that melted from the nearby heat source, Philadelphia Fire Commissioner Lloyd Ayres said. The heater then ignited the fuel, sparking the blaze, he said. The fire engulfed much of the first floor, but was quickly brought under control, authorities said.
Source: http://www.timesleader.com/mld/timesleader/news/local/134943 63.htm

[Return to top]

Defense Industrial Base Sector

6. *December 27, New York Times* — **Contractors are warned: cuts coming for weapons.** At a recent conference, Ryan Henry, a top Pentagon planning official, was giving an early glimpse of the Department of Defense's priorities over the next four years to an industry gathering in New York of executives of leading military contractors. Henry, principal deputy under secretary of defense for policy, said the Pentagon's spending binge of the last several years cannot be sustained. It was a message that the industry has been bracing for. The issue, however, goes beyond tightening budgets. Henry told the contractors that the Pentagon was redefining the strategic threats facing the United States. No longer are rival nations the primary threat −− a type of warfare that calls for naval destroyers and fighter jets. Today the country is facing international networks of terrorists, and the weapons needed are often more technologically advanced, flexible and innovative. He noted that special operations forces played a big role in the early days of the Iraq war and are expected to be used in greater numbers in the future. This would mean the Pentagon would want to buy more of the highly agile and high−technology weapons that they need. Specialized skills like language, intelligence and communication are also becoming top priorities.
Source: http://www.nytimes.com/2005/12/27/business/27weapons.html

[Return to top]

Banking and Finance Sector

7. *December 27, Associated Press* — **Florida strengthens state personnel system's security after complaint.** The security of Florida's new privately run personnel system is being strengthened after a complaint that confidential information on Governor Jeb Bush (R) and other top officials was compromised, the state announced Friday, December 23. The complaint from a former worker for Cincinnati−based Convergys Corp., which operates the system, alleged employees had for no legitimate reason repeatedly accessed confidential information on Bush, Attorney General Charlie Crist, Chief Financial Officer Tom Gallagher, and others. Investigators were unable to confirm any misuse of the data, according to a report by the Department of Management Services. The report also showed that home addresses, Social Security numbers, direct deposit information and other confidential material could be accessed, printed and e−mailed, and that the system lacked any way to track who had viewed it. The improvements include an automated tracking system of who accesses what information and

random computer audits to make sure sensitive data has not been downloaded. Access to confidential information will be limited to those who must have it to do their jobs.
Source: http://www.informationweek.com/showArticle.jhtml?articleID=1 75700290

8. *December 27, BetaNews* — **Spanish Trojan targets online bankers.** Antivirus firm Panda Software warned Tuesday, December 27, of a new Trojan that has begun to spread worldwide through MSN Messenger and attempts to obtain passwords of Spanish−speaking online banking users. Called Nabload.U, the Trojan actually downloads another, Banker.bsx, which is currently the most detected piece of malware by Panda's ActiveScan service. Nabload is different, however, in how it obtains the information. No keylogger is used, which means banks that have attempted to thwart Trojans by using virtual keyboards are not protected from this attack, Panda says. "This Trojan is an example of a hybrid virus that mixes different techniques. Once the user clicks on the URL, it is able to download a Trojan and use techniques similar to some spyware and phishing attacks," PandaLabs director Luis Corrons said.
Source: http://www.betanews.com/article/New_Spanish_Trojan_Targets_Online_Bankers/1135701236

9. *December 26, USA TODAY* — **New breed of cyberattack takes aim at sensitive data.** A new breed of targeted digital attack designed to steal sensitive data from computers at businesses and government agencies has emerged as the latest cyberthreat, tech security experts say. Organized crime groups in Eastern Europe and Asia are behind the attacks, which spy on the PCs of employees with access to highly sensitive data so they can steal bank account numbers, credit card numbers and other information, says Phillip Zakas, CEO of computer−security firm Intelli7. The targeted e−mails, launched through e−mail attachments containing malicious code, often appear to come from business associates and are hard to spot, he says. When opened, the attachment installs a small program on the victim's PC that downloads more malicious code and copies sensitive data. "These new attacks are corporate espionage," says Patrick Hinojosa, chief technology officer at antivirus firm Panda Software. The twist in attacks illustrates efforts by crooks to get at information through key insiders rather than scattershot with thousands of e−mails, says Neil MacDonald, security analyst at Gartner. Cybercrooks have narrowed their targets because of the effectiveness of computer−security software and hardware in tracing broader virus attacks.
Source: http://www.usatoday.com/money/industries/technology/2005−12−26−cyber−attack−usat_x.htm

10. *December 24, CNET News* — **Visa deals with possible data breach.** Visa USA acknowledged Saturday, December 24, that a U.S. merchant "may have experienced a data security breach" that compromised credit card account information. The statement came in response to a News.com inquiry related to customers whose Visa debit cards had been put on fraud watch or deactivated due to a security breach. In its statement, Visa said that after it learned "of the compromise, Visa quickly alerted the affected financial institutions to protect consumers through independent fraud monitoring and, if needed, reissuing cards." A Visa representative said Saturday that no other information was available at this time, including the name of the merchant, the number of accounts involved or when the event occurred.
Source: http://news.com.com/Visa+deals+with+possible+data+breach/2100−1029_3−6007759.html

[Return to top]

Transportation and Border Security Sector

11. *December 27, New York Times* — **Transit union and MTA said to be near final deal.** The transit workers' union has scheduled a meeting of its executive board for 6 p.m. Tuesday, December 27, at which union leaders are likely to present a final agreement with the Metropolitan Transportation Authority (MTA) for a new three−year contract. Approval by the executive board would be a major step toward ending the bitter contract dispute that resulted in a three−day transit strike last week. The strike was called off on Thursday afternoon, and the union returned to the negotiating table, after state mediators intervened. A settlement would still have to be ratified in a general vote of the union's membership. In announcing a framework to settle the strike, the mediators said on Thursday, December 22, that the authority had essentially agreed to drop its pension demands in exchange for the union agreeing to have its members pay more toward their health−care costs. Most current workers pay no premiums for the basic health plan.
Source: http://www.nytimes.com/2005/12/27/nyregion/nyregionspecial3/27cnd−mta.html?hp&ex=1135746000&en=7d4d20f2f7d11629&ei=5094& partner=homepage

12. *December 27, Associated Press* — **Florida mass transit driver charged with making bomb threat.** A mass transit driver was arrested Monday, December 26, after he allegedly threatened to blow up a bus, authorities said. An improvised bomb and two hollowed−out grenades were found in Victor Carrera's apartment. About 10 people in nearby homes were told to leave while a bomb squad searched the building, Broward County sheriff's spokesperson Jim Leljedal said. Police learned about the alleged threat from Carrera's relatives. Carrera, 40, was arrested at home before he could leave for work as a bus driver for Broward County Transit in south Florida, the sheriff's office said. He was charged with making a bomb threat, possession of a destructive device and possession of a hoax device. The sheriff's office said additional federal charges were possible.
Source: http://www.cbsnews.com/stories/2005/12/27/ap/national/mainD8 EOACG00.shtml

13. *December 27, Washington Times* — **Border initiative takes aim at smuggling corridor.** U.S. Customs and Border Protection has targeted the Del Rio, TX, sector for a multi−agency border−control initiative called "Operation Streamline II," which will focus on high−traffic smuggling corridors along the 205 miles of the Rio Grande that divide the sector from Mexico. "Securing our nation's borders from a potential terrorist threat and from the illegal entry of people, weapons and drugs is absolutely paramount," said U.S. Border Patrol Chief David V. Aguilar. The operation, involving the Border Patrol, U.S. Immigration and Customs Enforcement, the U.S. attorney's office and the U.S. Marshals Service, will focus on foreigners who enter the country illegally through high−traffic areas in the Del Rio Border Patrol sector. The plan calls for apprehended migrants who are not released on humanitarian grounds to be prosecuted for illegal entry, with a penalty of up to 180 days of incarceration. While the aliens undergo criminal proceedings, they also will be processed for removal from the U.S. The sector's 41 counties consist primarily of farms and ranches in a sparsely populated area −− making the region a major staging area for drug and alien smugglers.
Source: http://www.washtimes.com/national/20051227−120943−1582r.htm

14. *December 27, Associated Press* — **Worries grow about increasing number of birds at Alaska airport.** A growing bird population is prompting safety concerns among officials at the Juneau International Airport. Airport Superintendent Jerry Mahle blames the increase on the city shutting down its landfill incinerator. The airport already reports three to five incidents a year of aircraft hitting birds, he said. Mahle said a mini−assessment of the airport's bird problem is scheduled to begin this week. The airport is situated in the Mendenhall Wetlands, so birds have always been a problem, Mahle said. Pilots have long been warned about the abundance. But since Waste Management shut down its incinerators in June 2004, bird numbers around the airport have dramatically increased, Mahle said. Any aircraft/bird collisions are reported to the Federal Aviation Administration. A duck can damage the fuselage of a jet moving at 100 mph or more, Mahle said. A large bird, such as a crane or eagle, could cause even more damage. Mahle said the airport continues to use pyrotechnics, as well as coyote and owl effigies, to scare birds away. But that doesn't necessarily drive them away from the path of planes.
Source: http://www.usatoday.com/travel/news/2005−12−27−airport−birds_x.htm

15. *December 23, Transportation Security Administration* — **TSA finds security at Bandara Ngurah Rai International Airport does not meet international standards.** The Transportation Security Administration (TSA) on Friday, December 23, announced that the Bandara Ngurah Rai International Airport in Bali, Indonesia does not meet international security standards, and the department is taking action to warn travelers of this security deficiency. Based on an assessment by a team of security experts from TSA, the Department of Homeland Security (DHS) has determined that the airport does not currently maintain security measures consistent with the standards established by the International Civil Aviation Organization. In view of this finding, DHS has directed air carriers issuing tickets for travel between the United States and Indonesia to notify ticket purchasers of the identity of this airport in accordance with this determination. DHS also directed that the identity of this airport be displayed prominently at all U.S. airports and published in the Federal Register. The order is effective immediately. U.S. and foreign air carriers that fly directly between the United States and Indonesia are temporarily providing additional security measures that counter the deficiencies identified at the airport. Under Title 49 of the U.S. Code, Section 44907, DHS assesses security at foreign airports with direct service to the United States.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 019608c

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

16. *December 27, Stop Soybean Rust News* — **Several green kudzu patches infected with soybean rust in Alabama.** The first report of soybean rust in Mobile, AL, was last week on the

last two green leaves of a one−acre kudzu patch. Mobile, in southwest Alabama, is the 33rd county in the state and 138th in the U.S. with soybean rust this year. Ed Sikora, professor and Extension plant pathologist at Auburn University, said that the rust mentioned above was found on December 21. "We also detected rust on kudzu in two patches in Baldwin County, and one patch each in Conecuh and Clarke counties," he said.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=664

17. *December 26, RIA Novosti (Russia)* — **Russia's Far East steps up efforts to contain foot−and−mouth disease.** Veterinary officials in the coastal regions of Russia's Far East announced Monday, December 26, they would be toughening hygiene regulations to contain the spread of foot−and−mouth disease in the region. The measure comes in response to an outbreak of the disease at cattle farms in the Khabarovsk Area. All livestock and meat products leaving the area will now be subject to veterinary inspections, and a mass vaccination campaign is under way to protect livestock in neighboring regions. Officials also said the local population was being informed about symptoms, prevention and treatment of the disease, and had been advised to report all suspected cases to authorities.
Source: http://en.rian.ru/russia/20051226/42699502.html

18. *December 26, Associated Press* — **High fuel, fertilizer costs mean uncertainty for farmers.** The soaring cost of fuel and fertilizer carved deep into farmers' profits in 2005, and some worry the cuts may go even deeper in the new year. "We may be looking at a 40 to 50 percent reduction in net farm income just as a result of high fuel costs," North Dakota Agriculture Commissioner Roger Johnson said. "I think we're going to see some farmers go out of business." Good prices for wheat and record or near−record cattle prices helped farmers make money this year. But North Dakota suffered the second−largest scab disease−related loss in wheat and barley since 1997, and the worst outbreak of cattle anthrax in history.
Source: http://www.grandforks.com/mld/grandforks/news/13489867.htm

19. *December 24, Chattanoogan (TN)* — **Hunter charged under new chronic wasting disease law.** The Tennessee Wildlife Resources (TWR) has prosecuted its first case for a violation of an importation law that prohibits bringing cervid carcasses into Tennessee from states where local wildlife officials have concerns about chronic wasting disease (CWD). A Maury, TN, hunter charged in the case killed a mule deer in Nebraska, transported the carcass to Tennessee, and had the meat processed locally. He then took the head to a taxidermist to be mounted, according to the TWR. The law passed last year prohibits the importation, transportation, or possession in Tennessee of a cervid carcass, or carcass part, from states where CWD is known to have occurred. However, there are exceptions to the law provided specific precautions are taken. Those exceptions are mat that has had all bones removed, mat that has no portion of the spinal column or head attached, antlers attached to cleaned skull plates, finished taxidermy, and hides and or tanned parts. The Maury County hunter paid a fine for the violation, but was given the antlers, skull, and head after they had been cleaned.
CWD information: http://www.cwd−info.com
Source: http://www.chattanoogan.com/articles/article_77717.asp

[Return to top]

Food Sector

20. *December 26, Japan Economic Newswire* — **Japan confirms North American beef fulfilled import conditions.** North American beef met Japan's conditions for import resumption when a Japanese delegation inspected U.S. and Canadian meatpackers earlier this month, the government said Monday, December 26. Japanese officials inspected a total of 15 meat facilities in the two countries from December 13 −− the day after Tokyo lifted the ban imposed on North American beef due to concern about mad cow disease −− through Saturday, December 24. The facilities were in compliance with requirements set by Tokyo, such as the removal of specified risk materials and the age of cows at the time of slaughter, said the Ministry of Agriculture, Forestry and Fisheries and the Ministry of Health, Labor and Welfare. Japan, which banned the import of North American beef in December 2003, lifted the ban on December 12 on condition that the cows are aged 20 months or younger and spinal cords and other specified risk materials that could transmit mad cow disease are removed.
Source: http://www.tmcnet.com/usubmit/2005/dec/1240229.htm

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

21. *December 27, Rockford Register Star (IL)* — **Illinois to test response to pandemic flu.** To better prepare its public health system for a potentially devastating influenza outbreak, Illinois plans to hold a series of exercises to test the strength of its response. The state has hired a consultant to develop the exercises and, in the spring, expects to work with local health departments, hospitals, and other response personnel to sharpen its response plan. The effort could complement the work of a coalition of public health agencies in the Rock River Valley. Since last spring, the Rockford Regional Health Council Infectious Disease Committee has been formulating its pandemic flu response plan. The group convened after the September 11, 2001, terrorist attacks to consider the risk of bioterrorism, then switched gears to consider pandemic influenza.
Source: http://www.rrstar.com/apps/pbcs.dll/article?AID=/20051227/NEWS0109/112270013/1004/NEWS

22. *December 27, Associated Press* — **Rural hospitals face doctor shortages.** Health care experts say physician recruitment and retention is a perennial problem in Arizona, but the stakes are much higher in rural areas as the state's population soars. According to the Arizona Hospital and Healthcare Association, Arizona ranks among the states with the lowest number of working nurses and physicians per capita. Even more troubling is that according to the National Rural Health Association, one out of 10 of the nation's doctors practice in rural areas, where one−fourth of the nation's population lives. One of the challenges residents and physicians face in rural health care is the lack of specialists, placing the burden on rural doctors to fill in the gaps of knowledge and develop an eye for the subtle nature of life−threatening ailments.

Attracting primary−care physicians has also been a problem, said Alison Hughes, director of the Rural Hospital Flexibility Program at the University of Arizona. Hughes says that if a medical resident comes from a rural community, he or she is much more likely to practice in such a community. That means medical schools need to recruit rural students more vigorously.
Source: http://www.cbsnews.com/stories/2005/12/27/ap/health/mainD8EO IH3O0.shtml

23. *December 26, Reuters* — **China to launch new bird flu vaccine for poultry.** China will begin mass−production of a new bird flu vaccine for poultry by the end of the month that could also help in the development of a vaccine to protect people, state media said on Monday, December 26. The new vaccine −− one billion shots of which are expected to have been produced by year−end −− will be used alongside existing vaccines from next year, the China Daily said, quoting chief veterinarian Jia Youling. The live vaccine, which will also work against another poultry disease, exotic Newcastle disease, can be delivered orally, nasally, or by spraying and will cost a fifth of existing inactivated vaccines, the newspaper said. Standard flu shots are inactivated, meaning the virus is killed, but live vaccines contain weakened forms of the live virus. There have been 141 confirmed human cases of the H5N1 strain of bird flu in Asia, including six in China. Two people have died from bird flu in China, out of 73 known fatalities in Asia. Scientists fear the strain could mutate from a disease that largely affects birds to one that can pass easily between people, leading to a human pandemic.
Source: http://abcnews.go.com/US/wireStory?id=1442634

24. *December 26, National Institute of Allergy and Infectious Diseases* — **Researchers show how promising tuberculosis drug works.** Scientists from the National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health, have determined how a promising drug candidate attacks the bacterium that causes tuberculosis (TB). “PA−824, now in early stage clinical trials, holds promise for shortening the TB treatment regimen, which is currently cumbersome and lengthy,” says NIAID Director Anthony S. Fauci. In preclinical testing, PA−824 showed evidence of being effective against both actively dividing and slow−growing M. tb, giving rise to optimism that the compound may be useful in treating both active and latent TB.
Source: http://www3.niaid.nih.gov/news/newsreleases/2005/tbdrug.htm

[Return to top]

Government Sector

25. *December 27, Journal Standard (IL)* — **Security upgrades almost finished at Illinois county buildings.** Local law enforcement officials are nearly finished implementing several major security improvements at the Stephenson County Courthouse, public safety building and Freeport police station, according to Sheriff David Snyders. The upgrades are being made possible through a $90,000 grant from the Illinois Law Enforcement Alarm System recently received by the sheriff's office, in partnership with the Freeport Police Department. According to Snyders, the security improvements include duress systems, controlled access doors and video surveillance systems. Snyders predicted that the new systems will all be on line in less than a month. The duress system, which is for the courthouse and police station, has been installed, Snyders said. The system includes panic duress buttons that are placed in courtrooms, county offices and certain rooms at the police station. When the buttons are activated, a signal

is broadcast directly over a police radio frequency, letting authorities know that a specific office needs help, Snyders said. The controlled access doors and video surveillance systems are for all three buildings, and are in various stages of completion, officials say. Snyders said the county is still finishing up final programming work for the controlled access doors at the courthouse and public safety building.
Source: http://www.journalstandard.com/articles/2005/12/27/local_new s/news02.txt

[Return to top]

Emergency Services Sector

26. *December 26, Boston Globe* — **Drill reveals problems in terror response.** Terrorism preparedness exercises conducted in Boston, MA, in late spring showed that local law enforcement agencies are lacking in several areas, city officials said Sunday, December 25. According to a report issued late last week, local and State Police did not work together effectively because of confusion over who was in charge, and ambulances were delayed from reaching the mock scene at Logan International Airport. Mismatched computer programs also hindered the "Operation Atlas" response efforts. Metro Boston Homeland Security Region, an interagency task force, simulated a plane hijacking during several table−top exercises and one real−time drill. Some of the problems, including the mismatched computer systems, have been fixed, said Seth Gitell, spokesperson for Mayor Thomas M. Menino.
Source: http://www.boston.com/news/local/massachusetts/articles/2005 /12/26/drill_reveals_problems_in_terror_response/

[Return to top]

Information Technology and Telecommunications Sector

27. *December 27, TechWeb News* — **'Leaked' Windows Live Messenger really a Trojan.** F−Secure told users to ignore instant messages with the subject head "MSN Messenger 8 Working BETA" that go on to claim that "Messenger 8 BETA has been leaked!" The message, which refers to an alternate name for the upcoming Live Messenger, also contains a link. Users who click on the link, then download and run the executable file, are in reality installing the Virkel.f Trojan. Virkel.f adds the compromised machine to a botnet, from which the hacker can update the Trojan with additional malicious code, to make the PC into a spam zombie or along with others, launch a denial−of−service attack on Websites. Virkel.f also shuts down anti−virus and security software, and blocks access to sites that belong to security vendors. This bot worm spreads by hijacking IM contact names from an infected computer, then spimming those names with new messages about the "leaked" client.
Source: http://www.crn.com/sections/breakingnews/breakingnews.jhtml? articleId=175700348

28. *December 26, Secunia* — **Golden FTP Server APPE command buffer overflow vulnerability.** A vulnerability in Golden FTP Server can be exploited to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the handling of the "APPE" FTP command. This can be exploited to cause a buffer overflow by supplying an overly long argument. The vulnerability has been confirmed in version 1.92. Other versions

may also be affected. Secunia reports that the problem can be avoided by using the product only when connected to trusted networks.
Source: http://secunia.com/advisories/18245/

29. *December 24, FrSIRT* — **Sun Solaris PC Netlink "slsadmin" and "slsmgr" local vulnerabilities.** Two vulnerabilities were identified in PC Netlink for Solaris, which could be exploited to obtain elevated privileges. These flaws are due to errors in the "/etc/init.d/slsadmin" script and the "/opt/lanman/sbin/slsmgr" command that allow files to be opened insecurely, which could be exploited to write to the filesystem with the permissions of the user running "slsadmin" or "slsmgr", and execute arbitrary commands with "root" privileges (when "slsadmin" or "slsmgr" are run as "root"). Affected products are PC NetLink 2.0 (for Solaris SPARC 7, 8 and 9). FrSIRT reports that a solution is available; apply patches 121332−01 and 121209−01.
Solution: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1−21−121332−01−1
Solution: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1−21−121209−01−1
Source: http://www.frsirt.com/english/advisories/2005/3083

30. *December 24, Security Tracker* — **PC NetLink 'slsadmin' unsafe temporary files lets local users gain elevated privileges.** A vulnerability was reported in PC NetLink in the 'slsadmin' command. A local user may be able to gain elevated privileges on the target system. The '/etc/init.d/slsadmin' command in PC NetLink 2.0 opens files in the '/tmp' directory in an unsafe manner. A local user can cause arbitrary information to be written to the filesystem with the permissions of the user running 'slsadmin'. As a result, the local user can cause arbitrary code to be executed. A local user can write files to execute arbitrary code on the target system. The code will run with the privileges of the target user running 'slsadmin'. Security Tracker reports that a solution is available for PC NetLink 2.0 (for Solaris 7, 8 and 9) with patch 121332−01 or later.
Solution: http://www.sunsolve.sun.com/search/document.do?assetkey=1−26 −102117−1
Source: http://securitytracker.com/alerts/2005/Dec/1015409.html

31. *December 24, Security Tracker* — **PC Netlink 'slsmgr' unsafe temporary files lets local users gain elevated privileges.** A vulnerability was reported in PC NetLink in the 'slsmgr' command. A local user may be able to gain elevated privileges on the target system. The '/opt/lanman/sbin/slsmgr' command in PC NetLink 2.0 opens files in the '/tmp' directory in an unsafe manner. A local user can cause arbitrary information to be written to the filesystem with the permissions of the user running 'slsmgr'. A local user is then able to write files to execute arbitrary code on the target system. The code will run with the privileges of the target user running 'slsmgr'. Security Tracker reports that a fix has been issued for PC NetLink 2.0 (for Solaris 7, 8 and 9) with patch 121209−01 or later.
Solution: http://sunsolve.sun.com/search/document.do?assetkey=1−26−102 122−1
Source: http://securitytracker.com/alerts/2005/Dec/1015408.html

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a third party report of multiple heap buffer overflows in the Symantec RAR decompression library (Dec2RAR.dll). Although there is limited information concerning this reported vulnerability, US−CERT encourages users and system administrators to consider filtering or disabling the scanning of RAR archives at email or proxy gateways. However, disabling RAR scanning may compromise the effectiveness of the security product. In addition, blocking RAR archives may prevent legitimate information from entering the network. By using a specially crafted RAR archive, a remote attacker may be able to perform any of the following malicious activities:

Execute arbitrary code, possibly SYSTEM privileges

Cause a denial of service condition, possibly disabling antivirus capabilities

Take complete control of a vulnerable system

More information can be found in US−CERT Vulnerability Note VU#305272,Symantec RAR decompression library contains multiple heap overflows, at URL: http://www.kb.cert.org/vuls/id/305272

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4142 (oidocsvc), 27015 (halflife), 445 (microsoft−ds), 6881 (bittorrent), 25 (smtp), 32789 (−−−), 80 (www), 139 (netbios−ssn), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

32. *December 27, Manteca Bulletin Online Daily Newspaper (CA)* — **Burglars steal $10K in agricultural shop loot.** Burglars stole $10,000 worth of equipment from Manteca's East Union High's agricultural department over the holiday weekend. It was the second major burglary at the Ag complex in three months. Ag teacher John Hooper discovered the break−in shortly before noon Monday, December 26, when he went to the school to pick up a small motor he was going to use to draw a schematic. Manteca Police Corporal Randy Chiek said it appeared the thieves had driven in between classroom buildings after lifting one gate off its hinges. He questioned why night lighting in the area was not in use so that figures on the surveillance camera could be better identified. Among the items taken were red bolt cutters, Craftsman paint

spray gun, black Altrade chisel set, a Dewalt jig saw, a 3/8 drive silver impact gun, a portable Black & Decker band saw, a set of livestock management material, two Esag plasma cutters, a Dell laptop computer, five Husky ratchet sets, Hewlett−Packard Photo Smart printer, a yellow Dewalt hand drill, a red Milwaukee grinder, a Kodak Easy Share digital camera, a green and black Hitachi grinder, a black Jackson digital welding helmet, and a black Jackson full face welding helmet with gold lens.
Source: http://www.mantecabulletin.com/articles/2005/12/27/news/news 1.txt

33. *December 27, Channel 3000 (WI)* — **FBI investigates pipe bomb blast.** A pipe bomb exploded in a Madison, WI, parking ramp on Saturday, December 24. The FBI is now investigating the explosion, which occurred shortly after noon, when a man returned to his car to pay the meter. The bomb had apparently been placed on the tires of a car. When the driver returned and leaned up against the car, the bomb went off. This is the third time a bomb has been found in the same ramp since November, but the first time that one detonated. Madison police said that they wouldn't speculate on whether the three incidents are related. Madison police spokesperson Howard Payne said that the other two objects looked like bombs but turned out to be harmless. Madison police said that there are no plans to beef up security in the ramp until it receives more information from the FBI.
Source: http://www.channel3000.com/news/5674678/detail.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure

Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer